㈜이너버스
차세대 통합로그관리 시스템

2015.06.10

innerbus

CONTENTS

1. 로그란 ? / 로그 관리

2. 차세대 통합로그관리

3. 도입 필요성

4. 도입시 고려사항

5. 기대 효과

6. 구축 사례

innerbus

1. 로그란 ? / 로그 관리

로그(Log)란 전산 시스템 동작 중에 발생한 모든 내용
(누가, 언제, 어디서, 무엇을, 왜)에 대한 기록인
매우 중요한 자료(Data)이자 정보(Information)입니다.
LogCenter는 조직의 모든 IT기기에서 생성되는 이벤트 기록인 로그에 대해 수집, 분석, 저장, 폐기에 이르기까지 Life Cycle을 완벽히 관리를 통해 예방, 탐지, 추적, 대응 및 자산화를 실현할 수 있는 모든 기능을 제공하는
1등 기업이 사용하는 No 1. **차세대 통합로그관리 시스템**입니다.



예방 / 탐지 / 추적 / 대응
&
자산

1. 로그란 ? / 로그 관리

"**Log** - Immutable Fingerprint of User & Systems Activity"



innerbus

1. 로그란 ? / 로그 관리

"**구슬**이 **서말**이어도 **꿰어야 보배**다."





구슬 > 로그의 수집

- 수많은 로그 소스 (OS, Security, Network, DB, App. etc.)
- 서로 다른 포맷, 일반적이지 않은 형태
- 로그파일 수집 방식(Protocol) 대한 고민들
- 일관성 없는 Time Stamp

서말 > 로그의 저장과 보호

- 의도적, 비의도적 수정(변경) 및 삭제
- 이기종, 대용량, 장기간 보관에 따른 비용
- 무손실, 암호화 및 무결성
- Forensic & Compliance

꿰어야 > 분석과 Reporting

- 로그는 이해가 쉽지 않음 (복잡하고, 애매한 코드들의 산재)
- 낮은 우선순위, 담당자의 지식부족, 예방이 아닌 차후 대책 접근
- 분석방법의 혼재화 (모니터링, 검색, 상관분석, 시나리오분석 등)
- 기관(정부, 단체) 및 내부 보고서 작성의 어려움

보배 > Compliance, 정보(자산), 관리

- Compliance (법률, 가이드라인, 지침, 사규 등) 규정준수가 어려움
- 단순 누적 데이터로 정보화를 통한 자산화의 어려움
- Log LifeCycle 관리지침의 부재
- 환경변화(신규 도입, 암호화, 압축, 업그레이드 등)에 따른 관리의 어려움

2. 차세대 통합로그관리

로그관리, 이상징후탐지, 관제, Big Data를 위한 완벽한 플랫폼



1 시각화

- 역할기반 View
- 맞춤형 관제
- 토폴로지 Map

2 강력한 분석

- 상관관계 분석
- 실시간 탐지
- Smart Report

3 체계화

- 자동화된 로그관리
- Cloud 패치관리
- LFR에 의한 연동

4 편리한 사용성

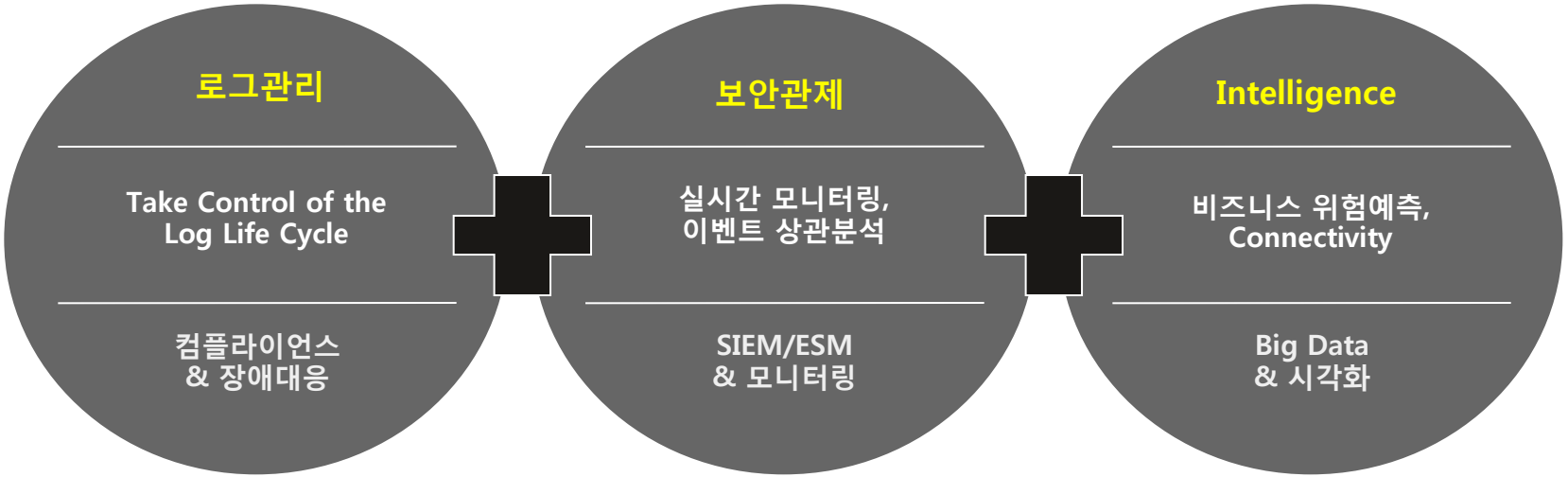
- 자연어 검색
- 공유 및 협업
- Widget Market

※ ***LFR : Log Format Regulation***

2. 차세대 통합로그관리

기업의 IT 인프라에 대한 데이터와 최근의 위협은
폭발적으로 증가하고 있습니다.
이에 대응하여 통합로그관리, 이상징후탐지, 실시간 관제를 융합한 진화된 **차세대 IT Intelligence** 기반의 **통합로그관리** 솔루션을 요구합니다.

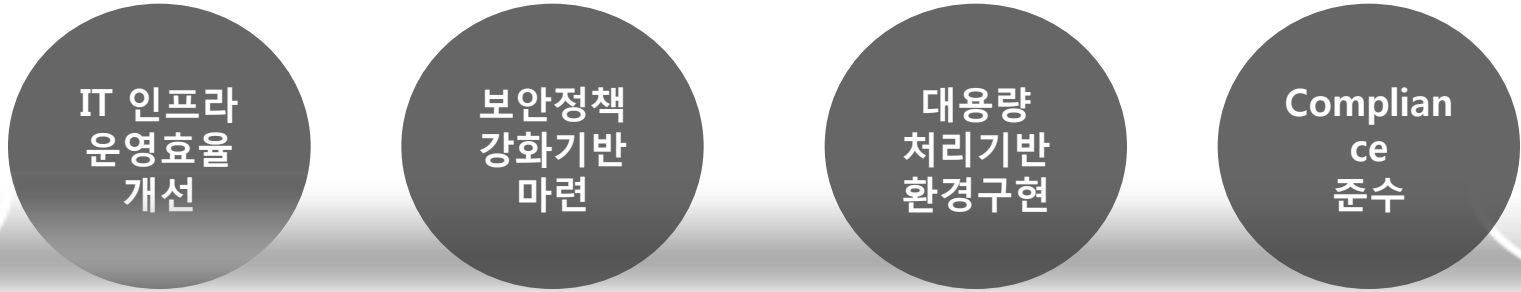
도전과제	Compliance 준수	Intelligence 확보	위협의 증가



innerbus

3. 도입 필요성

컴플라이언스 준수, 체계적인 로그 통합관리 및 실시간 모니터링 환경 구현



IT 인프라 로그 통합 관리

- 서버, 보안, 네트워크, 어플리케이션 등 이기종 시스템에 대한 로그 관리 필요
- 이기종 로그에 대한 중앙집중관리 필요
- **주요 로그의 실시간 수집 및 분석 필요**

실시간 분석 및 모니터링

- 필요 시 로그를 즉시 검색하고 보고서 생성 및 **상관분석 기능** 필요
- 대시보드를 통한 침해사고 예방 및 위협 관리와 시스템 모니터링 필요
- 실시간 알림을 통한 장애 대응 시간 단축 필요

대용량 로그처리 및 고속검색

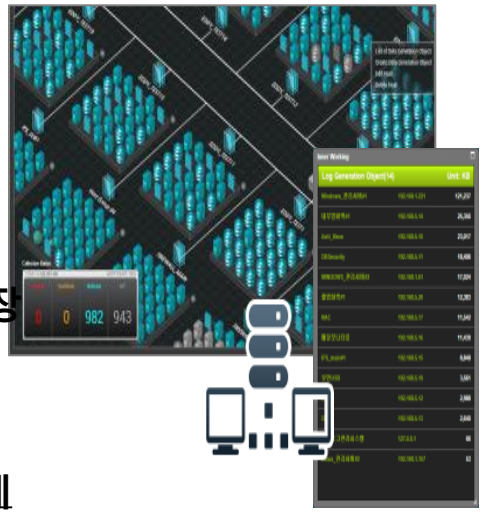
- 안정적인 대용량 로그의 수집 및 저장 필요
- **대용량 로그의 효율적 관리를 위한 고속검색 지원 필요**
- 장애 및 이상징후 발생 시 즉각적인 대처를 위한 **고성능 필요**

Compliance 준수

- 개인정보보호법, 정보통신망법 등 **법적 의무사항 준수** 필요
- 저장 주기 적용한 로그의 위변조 방지 저장 및 모니터링 및 보고 진행 필요

4. 도입 시 고려사항 (수집, 저장)

IT 인프라에 존재하는 모든 종류의 로그파일을 보안, Compliance, 운영목적에 맞게 관리하는가 ?



Compliance 준수

데이터 수집

원본로그 **압축, 암호화** 후 위변조방지,
인덱싱데이터는 **HICF(압축파일)로 저장**
로그파일 자동 생명주기 관리

Agentless, Agent, 실시간, 배치수집
Syslog, FTP, SNMP, ODBC 지원
정형, 비정형데이타 수집



시스템 최적 연계

단일장비 일 200GB 처리 **아키텍처**
Topology Map 상에서 로그연동
Unified Data Capture(정규화)

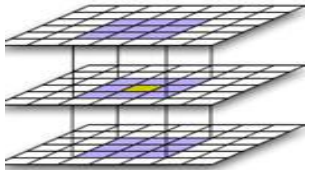
innerbus

4. 도입 시 고려사항 (분석구조)

분석은 100% **Full Text Indexing** 후 검색, 탐지, 보고
및 모든 로그에 대한 완벽한 활용성을 보장하는가 ?


정규화




HICF

Hyper Index
- Contextualize
- 100% Full Text

Hyper Search
- 초당 수GB 분석
- Group, Join, Multi

Intelligence
- 자연어 검색
- 추천 검색

단일 포인트에서 모든 분석


검색

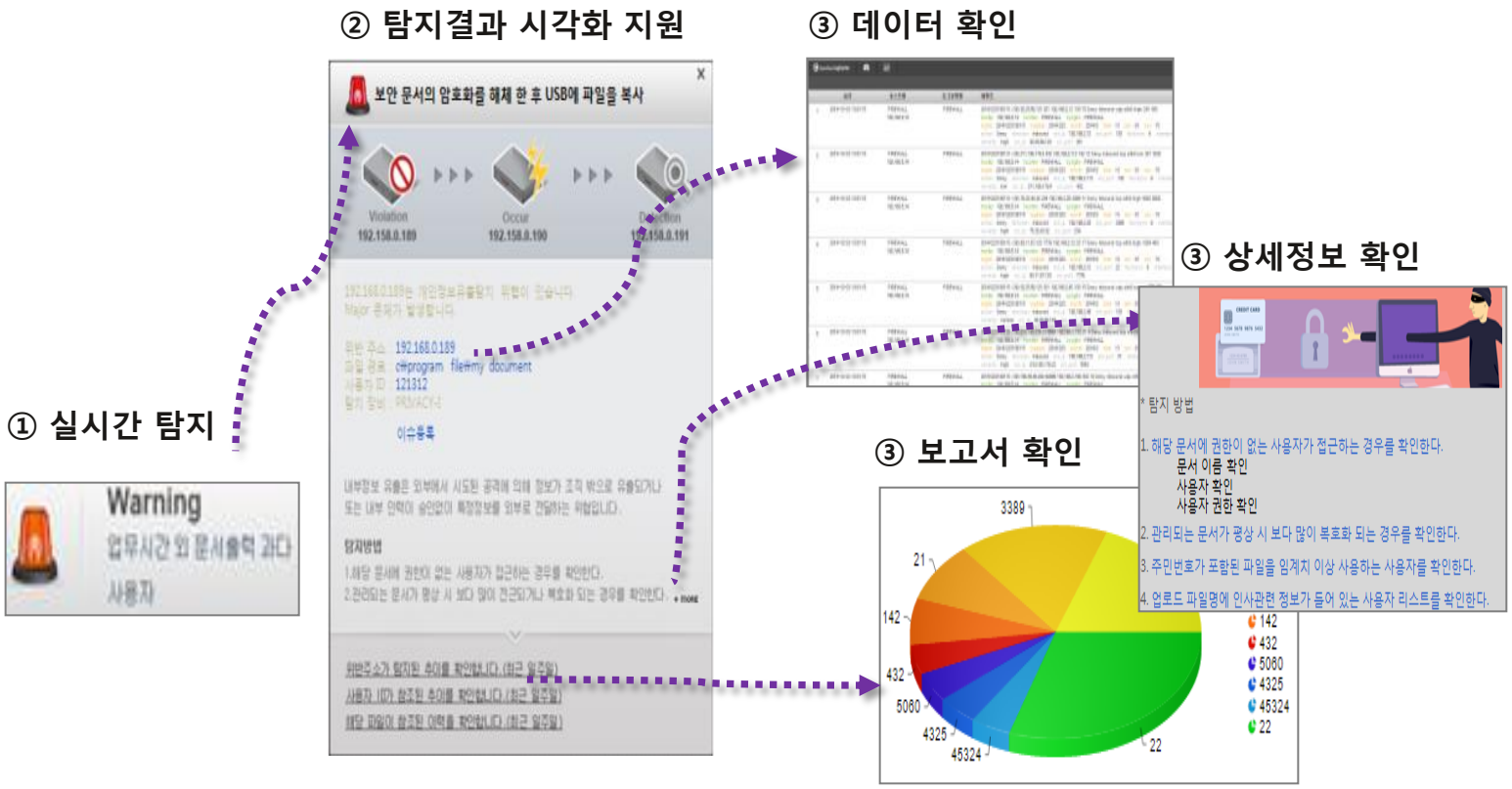

탐지


보고

※ HICF(Hyper Index Compress File)

4. 도입 시 고려사항 (실시간 탐지)

정책(Rule)기반 실시간 탐지 및 사전 모니터링을 활용하여
이상징후, 장애에 대한 완벽한 Insight를 제공하는가 ?



innerbus

4. 도입 시 고려사항 (Dashboard)

비즈니스 관점의 사용자 정의형 UX를 적용하여 역할별 탐지 및 관제기능을 포함하고 있는가 ?

- ✓ 다양한 관제에 적합한 직관적 UX Platform 적용
- ✓ Widget Market을 통한 최적의 맞춤형 컨텐츠 제공
- ✓ 검색, 위젯, 템플릿으로 커스터마이징 작업 지원
- ✓ 전체운영, 서버, 방화벽 전용 Topology 제공
- ✓ Google Map 및 World Map 제공



innerbus

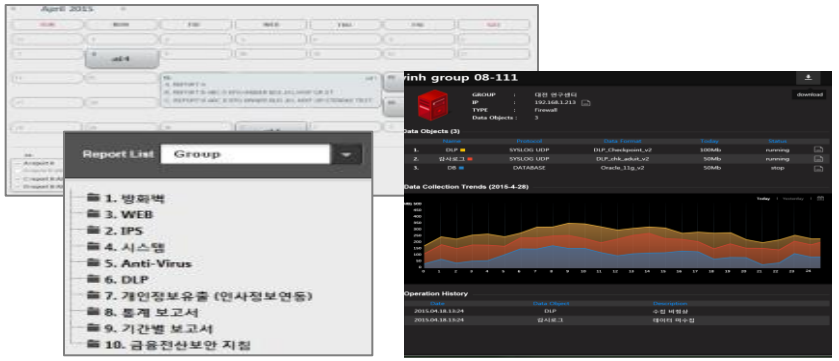
4. 도입 시 고려사항 (Report)

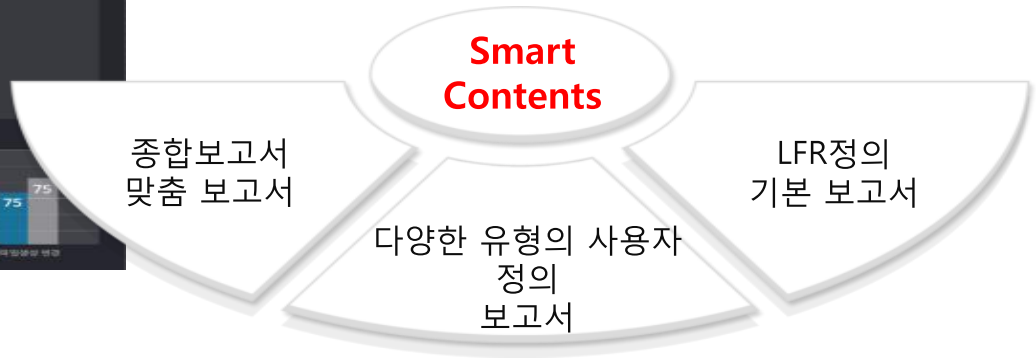
언제, 어떤 대상, 어느 상황, 누구에게 보고하든
Smart Contents Report를 제공하는가 ?

✓ 종합보고서



✓다양한 보고서





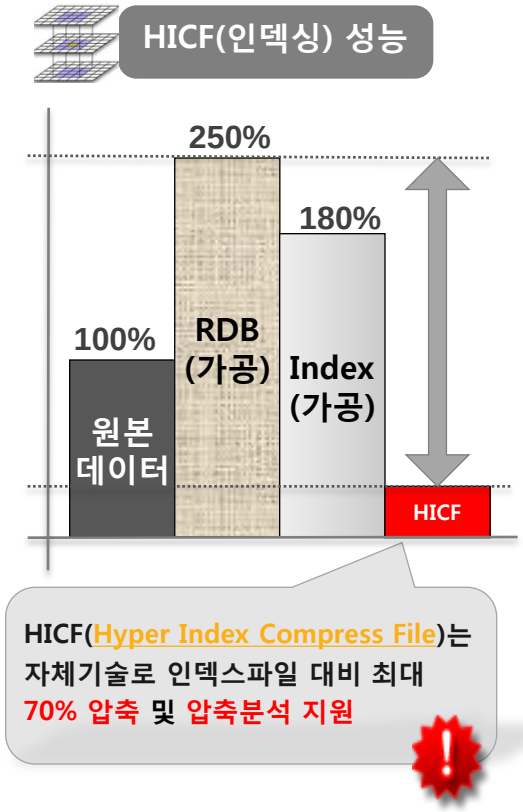
※ LFR : Log Format Regulation

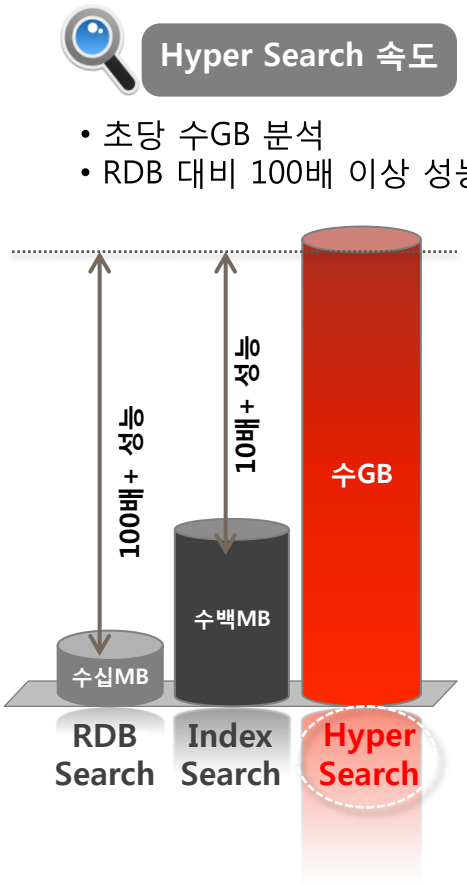
innerbus

4. 도입 시 고려사항 (권한관리 & 성능)

분석데이터 활용을 위한 **성능 보장**과 메뉴, 대상 등의 권한관리와
이슈 발생 시 유관부서와 시스템을 통해 **소통 및 조치(협업기능)**
할 수 있는가 ?



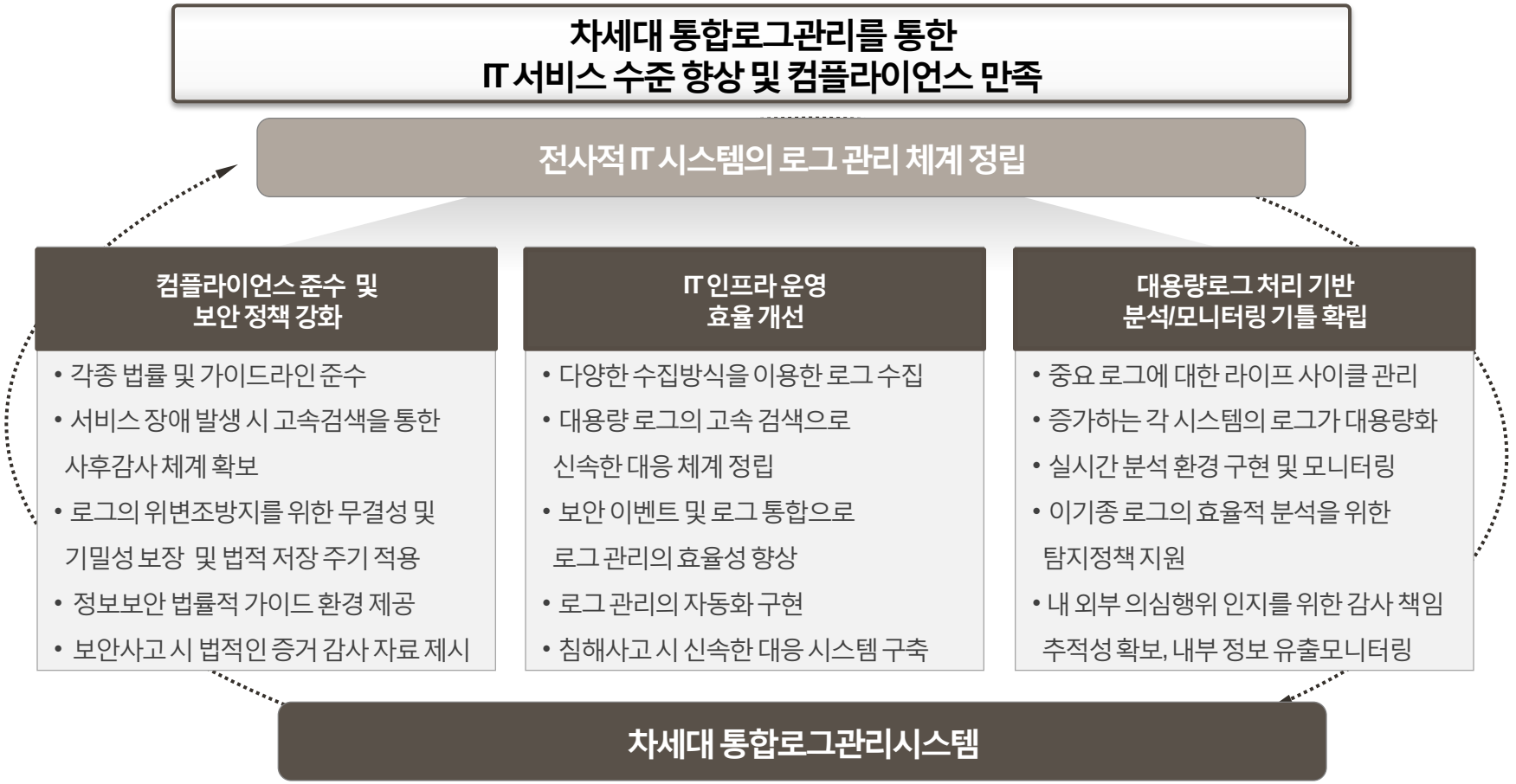




innerbus

5. 기대효과

LogCenter는 로그 수집, 분석, 모니터링, 관제에 이르는 완벽한 LogLifeCycle 관리 뿐만 아니라 **규정준수를 충족**하고 정보유출 및 이상징후 모니터링을 통하여 보안사고를 신속히 대응할 수 있는 통합로그 관리 체계를 정립합니다.



6. 구축 사례

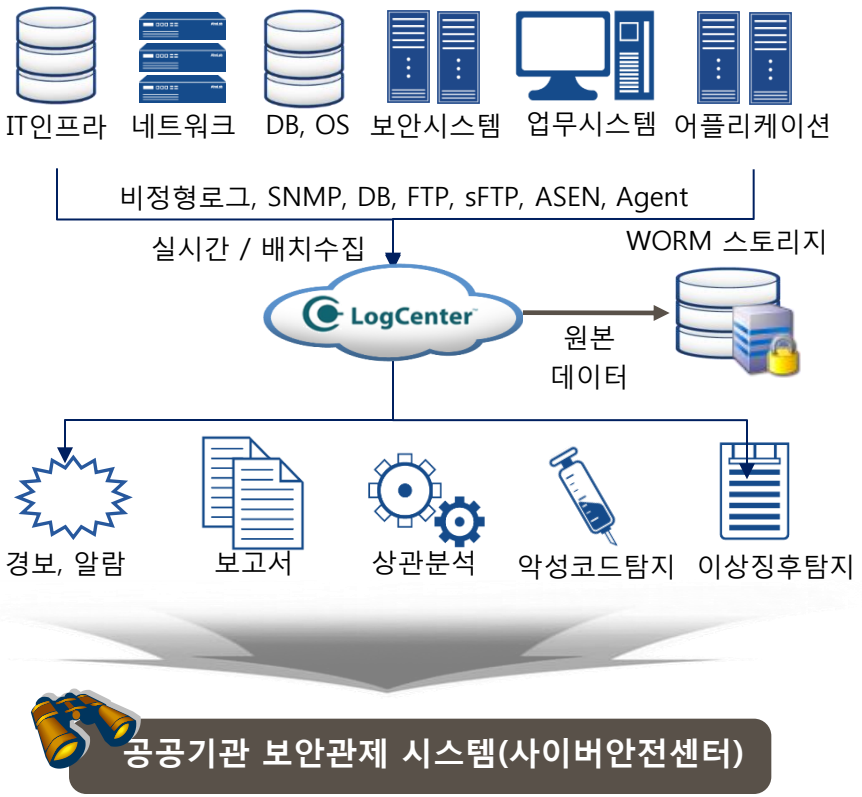
A社에서 발생되는 대량의 보안이벤트 로그 정보를 수집, 보안관제 시스템 및 사이버안전센터와 연계하여 컴플라이언스 준수 대응 및 로그분석을 지원하는 솔루션을 구축하였습니다.

A 社

1일 로그량 100GB

로그생성객체 150EA

주요 로그 생성 객체
서버(OS, DBMS 등), N/W, 보안솔루션 등



- ✓ 대용량 로그의 저장 및 관리
- ✓ 사이버 안전센터와의 연계 분석 지원
- ✓ 컴플라이언스 준수 및 보안사고 체계 대응

innerbus

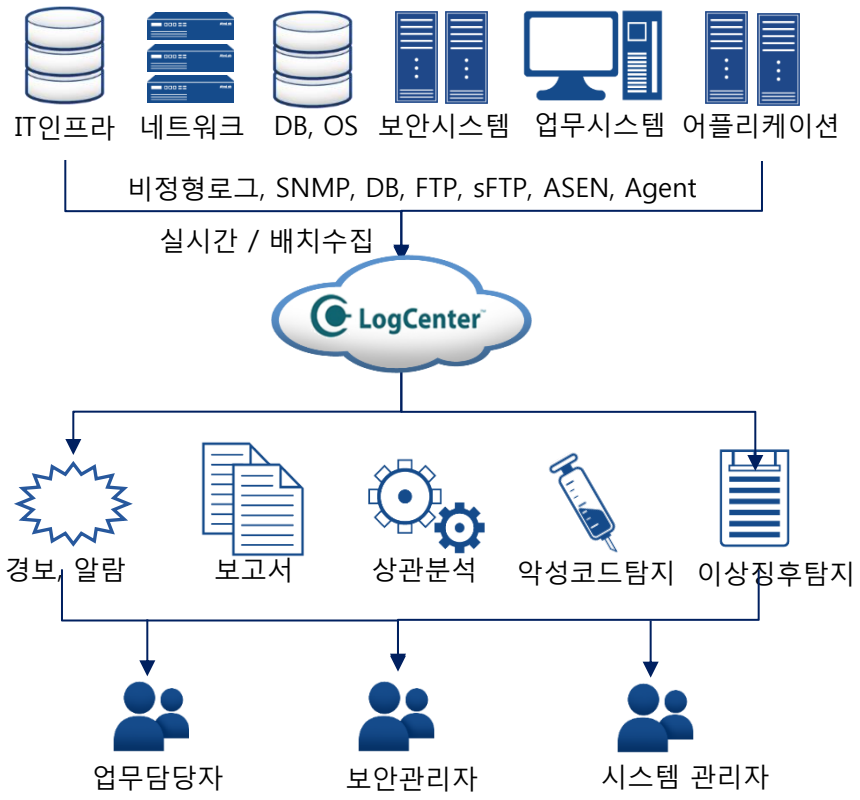
6. 구축 사례

B社에서 발생되는 서버, 네트워크, 보안시스템, 업무시스템 등 다양한 로그 정보를 수집하여 통합로그관리시스템 구축 완료 후, 탐지 정책 기반의 이상징후 탐지시스템으로 고도화를 수행하였습니다.

B 社



- ✓ 산재된 이기종 로그 통합 관리
- ✓ 보안사고 이상징후 실시간 탐지
- ✓표준 탐지 정책 수립 및 적용



innerbus

6. 구축 사례

C社에서 발생하는 대용량 로그기반으로 이상징후 탐지 및 전산사고 방지를 위한 대용량 로그관리와 상관분석 기반 모니터링 시스템을 구축하였습니다.

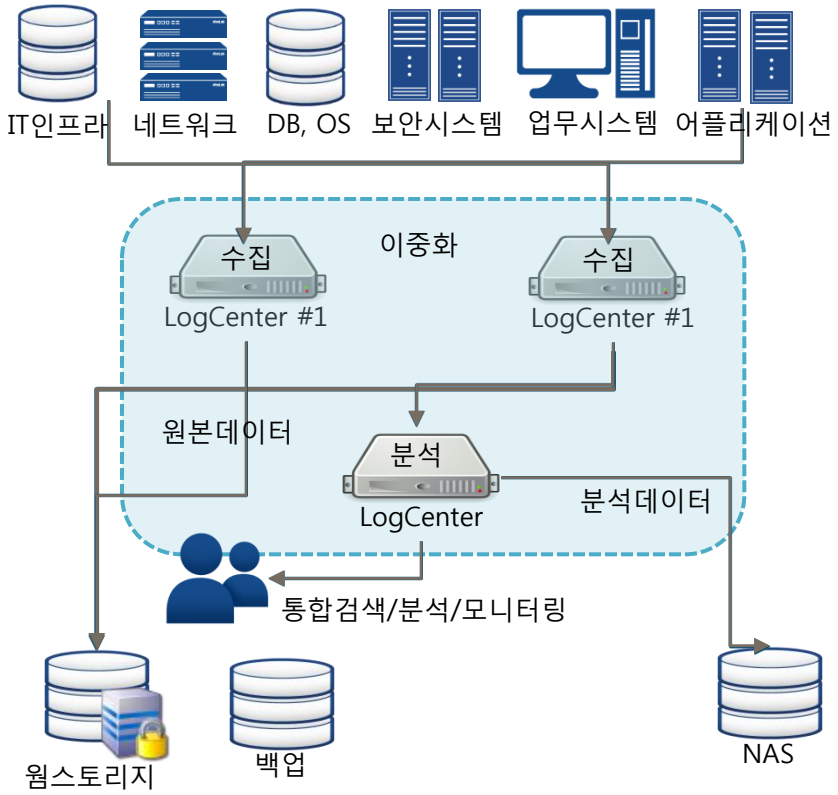
C 社

1일 로그량 150GB

로그생성객체 250EA

주요 로그 생성 객체
서버(OS, DBMS 등), N/W, 보안솔루션 등

- ✓ 대용량 로그의 저장 및 관리, 이중화
- ✓로그 데이터 분석을 통한 이상징후 탐지
- ✓ 의심행위 인지 및 사고 사후 법적 증빙



innerbus

Thank you

